Chiffrement de données multimédia:

Crypto-compression vidéo et standardisation

Cyril BERGERON (Thales)
Wassim HAMIDOUCHE (IETR)

Outline

Introduction : Video Encryption

- Context
- Current usage & Drawbacks

Selective Encryption

- Crypto-compression scheme

Standardization Activities in MPEG (ISO/IEC/JTC1/WG11)

- VIMAF
- Video Encryption Challenge

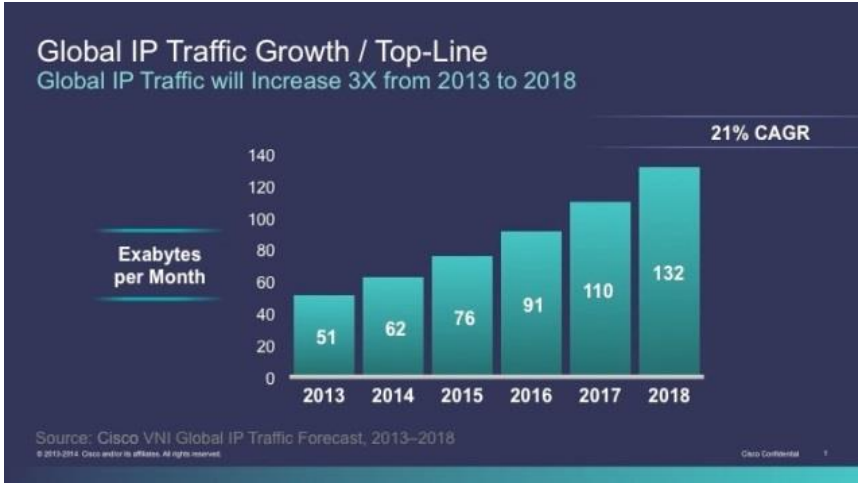
Conclusions

Video Encryption

THALES

Video traffic on the Internet (VNI-CISCO)

- IP traffic > 2 zettabytes in 2019,
- Connected devices: 3 x world's population,
- 22 Go consumed by capita,
- Videos represent about 80% of global Internet traffic.



Video Encryption

Currently, compression and encryption are two different and independent steps.

- **Compression** is set in the Video (or audio) coding layer,
- **Encryption** is applied on system layer.

In MPEG standards:

- **ISO/IEC 23001-7** (*Common encryption in ISO base media file format files*) and **ISO/IEC 23001-9** (*Common encryption of MPEG-2 transport streams*) define different modes and signaling of encryption for compressed stream.
- Current encryption scheme is based on "*blind*" ciphering a.k.a. Naive Encryption Algorithm '**NEA**' (ex: AES-CTR or AES-CBC) and treats the video bitstream as a **single text data**.

Video Encryption

Drawbacks of existing solutions:

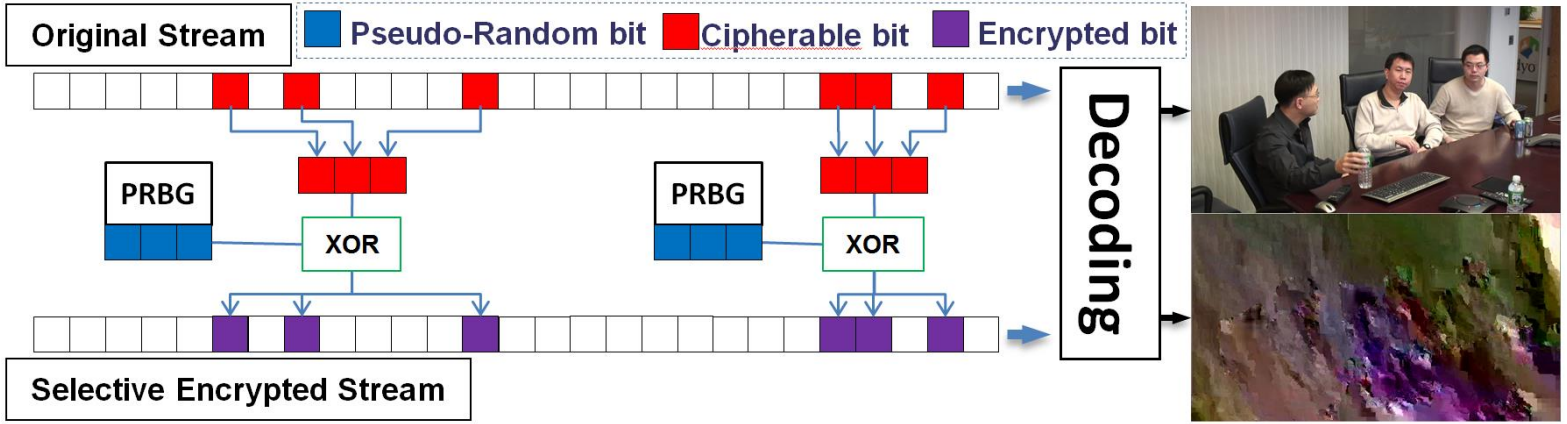
- **Cryptanalysis**: C. Shannon pointed out the fact there is a strong relationship between data compression and encryption. He demonstrated that removing redundancy in a source, could strengthen encryption.
  To be a perfect secured scheme, it supposes that the compressed data has no statistical redundancy.
  Moreover, in this current scheme, the "protected" stream cannot be interpreted by decoder, that can constitute a prior knowledge for **cryptanalysis attack**.
- **Network and error resilience** : With "Full encryption" scheme, it does not provide access to slice header or SEI NAL , which are necessary to transmit the data using a network protocol (like RTP) or to repackage Common Encrypted elementary streams between ISO media and MPEG-2 Transport Stream containers.
- **Complexity and delay**: Standard cypher brings a non-negligible computational complexity and delay. This aspect is currently a little managed by the option of "pattern encryption".

Selective Video Encryption

THALES

Selective Video Encryption

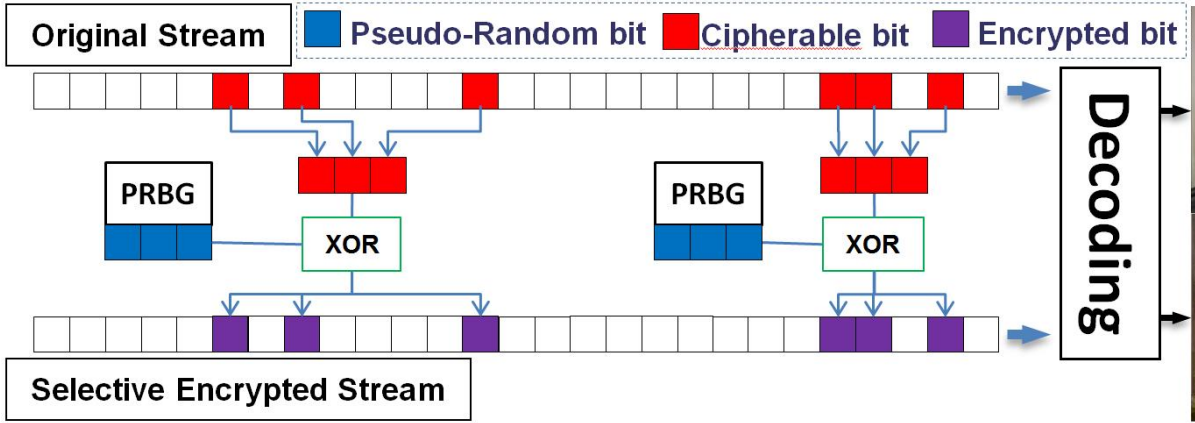
Selective Encryption Scheme (crypto-compression):

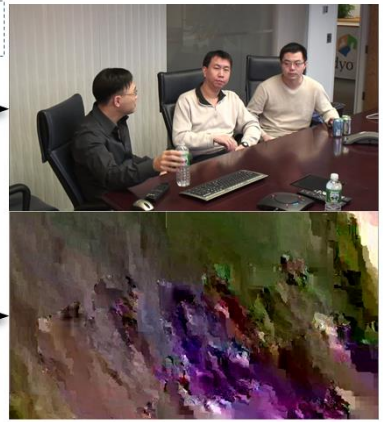


- the idea is to apply a ciphering that will alter the video stream only visually while keeping it **fully decodable** even by a non-robust standard compliant decoder, and without changing **compression efficiency**.
- Data to be ciphered is XORed with a ciphertext, which is generated by a Pseudo-Random Bit Generator (PRBG) like AES, Chaos-based Crypto Systems, etc.

Selective Video Encryption

Selective Encryption Scheme (crypto-compression):





- Example with exp-Golomb VLC codewords in H.264/AVC (CAVLC):
  - some bits could be 'modified' (i.e. **are Cypherable**) without modifying the interpretation of the rest of the bitstream.

Index	Slice_QP_Delta value	Codeword
0	0	1
1	1	010
2	-1	011
3	2	00100
4	-2	00101
5	3	00110
6	-3	00111
…	….	…

Selective Video Encryption

Selective Encryption Scheme (crypto-compression):

- Ex: Entropic coded Sequence of **13** symbols {-1,0,0,2,0,-3,-3,1,-1,1,0,0,0} with VLC, we obtain : [0111100100100111001110100110101111] (**34 bits**)
  - If we cipher **only** one bit we can obtain [0111101100100111001110100110101111] so it will be bad interpreted as {-1,0,0,**-1**,2,0,0,0,-3,1,-1,1,0,0,0} (**15** symbols)
  - If we cypher any bits '**cypherable**' (in the sense of selective encryption) we keep the compliancy and we do not create desynchronization (i.e. a misinterpretation for the rest of the bitstream):

[0**1**0110011**1**1001**00**0010**0**0110**1**10**1**0111] is interpreted as {**1**,0,0,**-3**,0,**2**,**2**,**-1**,**1**,**-1**,0,0,0} (**13** symbols)

Index	Slice_QP_Delta value	Codeword
0	0	1
1	1	01**0**
2	-1	01**1**
3	2	00100
4	-2	00101
5	3	00110
6	-3	00111
…	….	…

NB: here we have used a systematic XOR, normally we used a PRBG like AES with random bits

Selective Video Encryption

Selective Encryption Scheme (crypto-compression):

- Example from ‘Video Encryption Challenge’

Standardization Activities

Privacy Management in Multimedia Streaming Applications

- With the fundamental right to physical privacy (ex: US 4th amendment), it remains **the responsibility** of the cameras' owner and monitor to protect the access, the usage and the diffusion of media streams.
- The potential for personal data to be exploited for identity theft and other fraudulent activities has made it an attractive target for criminals. Consequently, personal data is the target of a significant proportion of **malicious** online activity, with criminals employing a range of technical and social engineering techniques in attempts to obtain personal data.
- Thereby, the access to video should be managed and controlled by the user, the video can only be viewed with a **limited access** that the user chooses: group of people, purpose of sharing, time, date, metadata, etc…
- Thus, there is a need to organize how it can be possible to give a conditional access to the total or a part of media data inside the video bitstream.

Privacy Management in Multimedia Streaming Applications

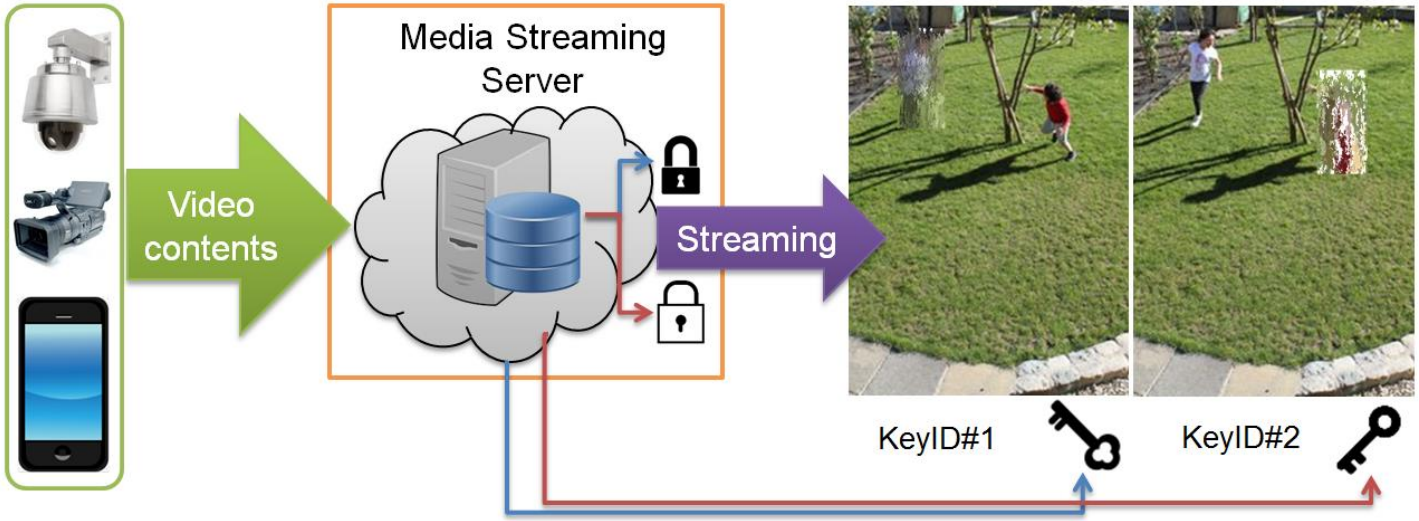
- Use cases for privacy protection:
  - CCTV (video surveillance): The video surveillance raises a challenge for **constitutional law.** The public movements could be displayed, but **identification** (faces,…) could be limited to people legally authorized
  - TV report: A TV report can **capture and broadcast** people who don't want to be filmed and don't want us to know where they were and what they did. Any publication on TV of the image of a person presupposes, in principle, **prior authorization** from the person concerned (or his legal representative).
  - Social Media: People can be on a picture or on a video taken by someone else, either **intentionally or by mistakes**, and such media can be posted on a social media service without any permission of the person who was captured.

Privacy Management in Multimedia Streaming Applications

- Existing solutions to provide privacy protection in video stream:
  - Blurring
  - Pixelization
  - Masking
  - Scrambling
  - Morphing

  They need additional information (for reversibility) and the compress ratio is modified
  - Full Encryption (but it is not possible to have a partial view of the video)
  - **Selective Encryption (*Content Sensitive Encryption*):**
    - **Compression Efficiency:** not affect the compression ratio (no additional information)
    - **Network friendliness:** System agnostic
    - Does Provides **Region encryption**
    - **Low complexity** adding

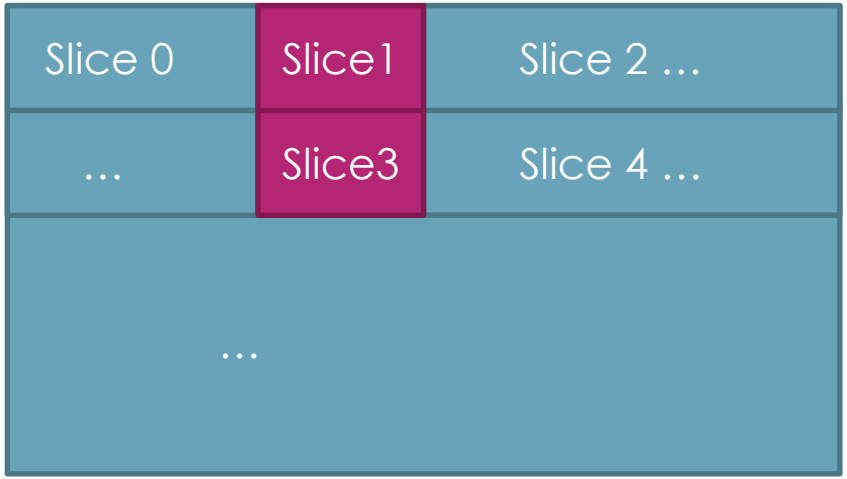
ISO/IEC 23000-21: MPEG-A Visual Identity Management Application Format



- Media should only be viewed with a well-defined limited access:
  - Some particular **regions** of the video could only be seen by the authorized users,
  - A need to manage different **control access** (i.e. different key identifiers).

ISO/IEC 23000-21: MPEG-A Visual Identity Management Application Format

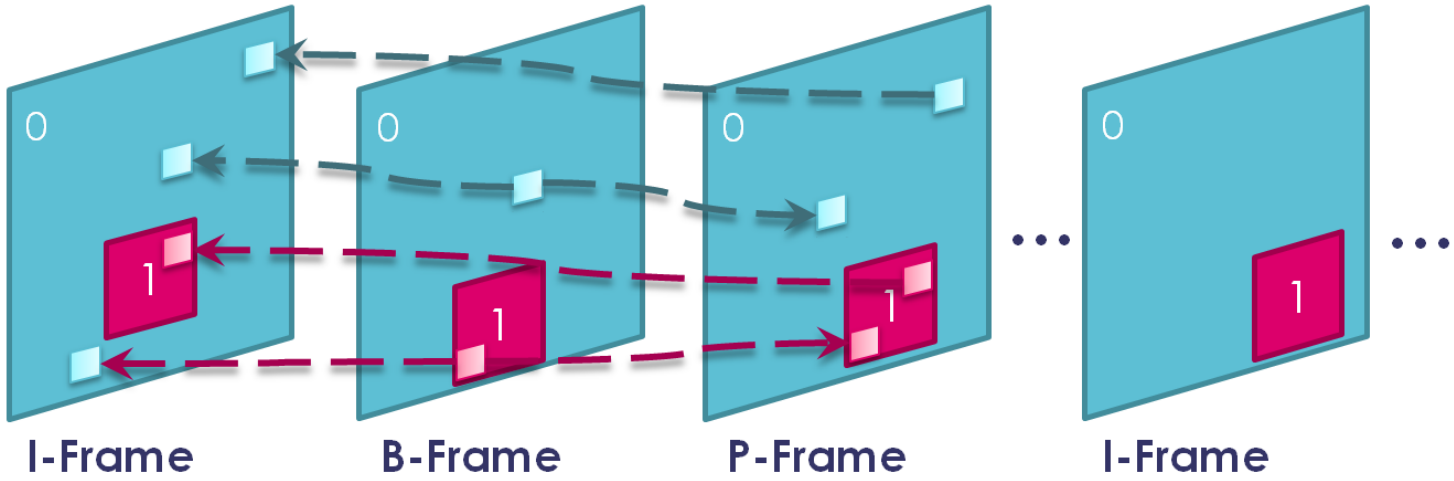
- Since the selective encryption takes place inside CODEC, it is also possible to restrain the selective encryption **locally**.



- Different tools are present in AVC and HEVC codecs to perform region encryption: Slices, Slice groups (AVC) and Tiles (HEVC)

ISO/IEC 23000-21: MPEG-A Visual Identity Management Application Format

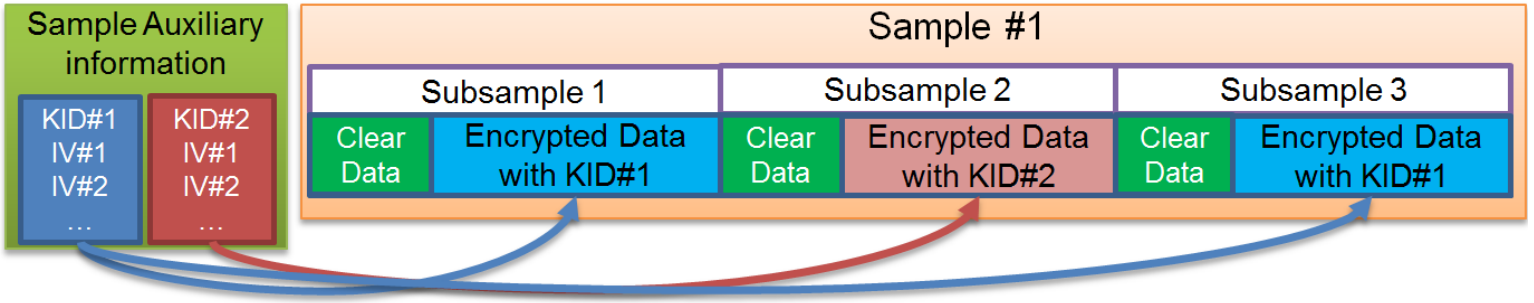
- Since the selective encryption takes place inside CODEC, it is also possible to restrain the selective encryption **locally and temporally**.



- To prevent **drift problem**, a non-cyphered region can not point (or refer) to a cyphered previous region.

ISO/IEC 23000-21: MPEG-A Visual Identity Management Application Format

- Encryption with Different Keys inside the same sample (ISOBMFF):



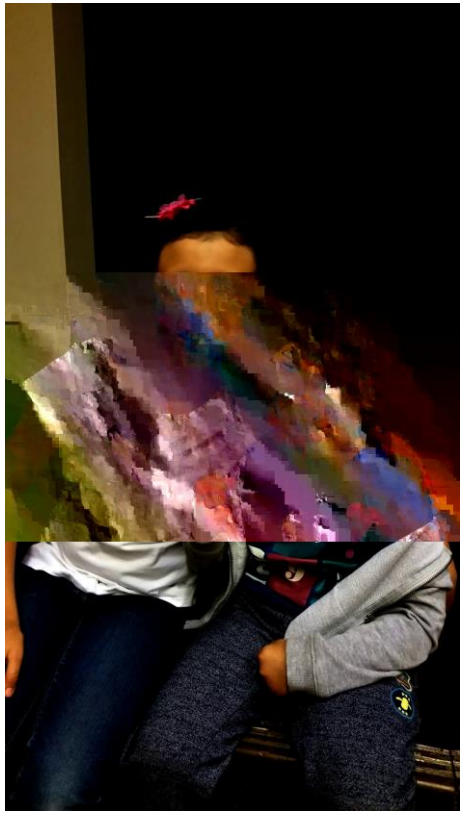
- it permits to manage multiple access for region encryption
- But media files may contain a mixture of encrypted and unencrypted samples.
- Modifications of **ISOBMFF** (ISO/IEC 14496-12 – MPEG-4 Part 12) and **CENC** (ISO/IEC 23001-7) are in progress.

Video Encryption Challenge

- For this challenge we provide three HEVC and three AVC bitstreams which have been ciphered using different selective encryption methods to test the **robustness** of these solution against different types of attacks.
- We provide information on how to encrypt and encode the HEVC bitstreams ciphered with the selective encryption solutions using open source software. We also provide six ciphered AVC and HEVC bitstreams that can be used as reference for **security evaluation** of selective encryption.
- The detailed information related to the challenge can be found in the following website (Software & Bitstreams): **http://openhevc.insa-rennes.fr/press-release/avc-and-hevc-selective-video-encryption-decryption-challenge/**

Video Encryption Challenge

- Video Format: AVC & HEVC in MP4 (ISO/IEC 14496-12)
- Image Format: AVC & HEVC in HEIF (ISO/IEC 23008-12)
- Encoded with **Kvazaar** (*Tampere University of Technology*)
- Encapsulated with **GPAC** (*Telecom ParisTech*)
- Decypherable with **openHEVC** (*IETR/INSA Rennes*)



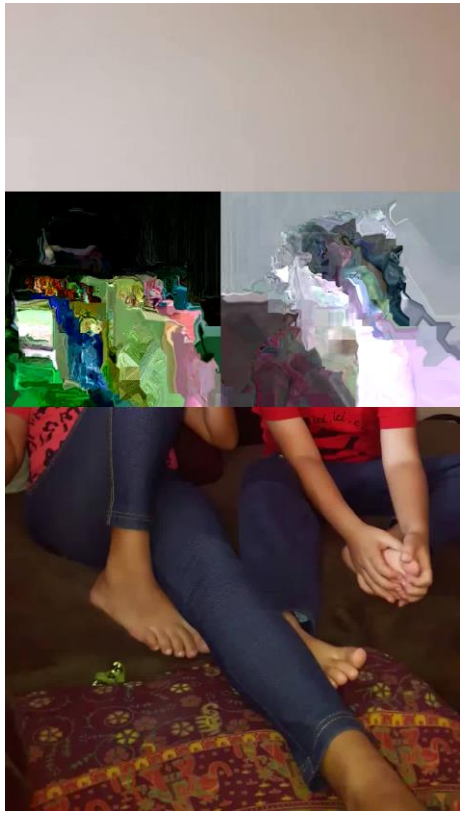


image Video

Conclusions

THALES

Conclusion

We currently standardized a complete ROI crypto-compression solution

- Protecting privacy in **HEIF**, **AVC** and **HEVC**,
- Encrypts only the **ROI** in the video and keeps the rest of the video unencrypted,
- The proposed **selective encryption** method is performed at the codec level,
  - The encrypted bit-stream is **decodable** with a standard compliant decoder,
  - A **privacy key** is only needed for ROI decryption,
- Initiate a **Video Encryption Challenge** to test robustness against cryptanalysis,
- It should be soon incorporated in :
  - **VIMAF** standard (ISO/IEC 23000-21)
  - **CENC** a.k.a **Common Encryption** standards (ISO/IEC 23001-7 and ISO/IEC 23001-9)

Questions

Thank you for your attention

Video Encryption Challenge:
http://openhevc.insa-rennes.fr/press-release/avc-and-hevc-selective-video-encryption-decryption-challenge/

Contact: cyril.bergeron@thalesgroup.com
wassim.hamidouche@insa-rennes.fr

THALES

Bibliography

References

- C. Bergeron, C. Lamy-Bergot, **"Compliant selective encryption for H.264/AVC video streams"** - *Proc. IEEE 7th Workshop Multimedia Signal Process.*, pp. 1-4, Oct./Nov. 2005.
- Z. Shahid, M. Chaumont, W. Puech, **"Fast Protection of H. 264/AVC by Selective Encryption of CAVLC and CABAC for I and P Frames"** - *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 21, no. 5, pp. 565-576, 2011.
- T. Stutz, A. Uhl, **"A survey of H.264 AVC/SVC encryption"** - *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 22, no. 3, pp. 325-339, March 2012.
- B. Boyadjis, M.-E. Perrin, C. Bergeron, S. Lecomte, **"A real-time ciphering transcoder for H.264 and HEVC streams"** - *Proc. IEEE Int. Conf. Image Process. (ICIP)*, pp. 3432-3434, Oct. 2014.
- W. Hamidouche, M. Farajallah, M. Raulet, O. Deforges, S. El Assad, **"Selective Video Encryption using Chaotic System in the SHVC Extension"**, *2015 IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP)*, pp. 1762-1766, 2015.
- M. Farajallah, W. Hamidouche, O. Déforges, S. E. Assad, **"ROI encryption for the HEVC coded video contents"**, *Proc. IEEE Int. Conf. Image Process. (ICIP)*, pp. 3096-3100, 2015.
- C. Bergeron , N. Sidaty , W. Hamidouche , B. Boyadjis , J. Le Feuvre , Y. Lim,**"Real-Time Selective Encryption Solution based on ROI for MPEG-A Visual Identity Management AF "**- *International Conference on Digital Signal Processing (DSP)*, pp. 1-5, 2017.